UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,313	11/12/2003	Peter M. Rothermel	248588002US1	8877

25096 7590 10/19/2007

PERKINS COIE LLP
PATENT-SEA
P.O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
10/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/712,313	ROTHERMEL ET AL.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,31-40,50,51 and 82-87* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,31-40,50,51 and 82-87* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/12/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the communication dated on 06 August 2007.

Election/Restrictions

2. Applicant elected without prejudice Species 1, claims 1-10, 31-40, 50-51 and 82-87.

3. Claims 11-30, 52-64, 69-71, 77-81, 88-90 and 95-101 corresponding to Species 2, 3, 4 and 5 are cancelled.

Claim Objections

4. Claim 1 is objected to because of the following informalities:

a. It recites "the manager device" in line 26; there is lack of antecedent basis for this limitation. It is assumed that the applicant intended to claim "the security manager device".

b. It recites "the information" in line 28. It is not clear if claimed information referring to "security control information" of line 9 or "network security information" of line 20.

Appropriate correction and/or clarification is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-4, 6-10, 31-32, 35, 37-40, 50-51, 82-83 and 86-87 are rejected under 35 U.S.C. 102(b) as being anticipated by Boyle et al. (Patent No.: 5,577,209) (hereinafter "Boyle").

7. As to claim 1, Boyle discloses a method for a security manager device to manage a plurality of network security devices with a plurality of supervisor devices, each network security device generating network security information related to an associated group of network devices, storing the generated network security information on a primary supervisor device for the network security device when the primary supervisor device is available to store the generated network security information, and storing the generated network security information on an alternate supervisor device when the primary supervisor device is unavailable (abstract), the method comprising:

distributing security control information to multiple network security devices, the security control information to be used to generate network security information (Boyle teaches this concept by having a Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to it's assigned SNIUs -e.g. col. 3, lines 30-42), by

determining a supervisor device that is the primary supervisor device for each of the multiple network security devices (Boyle Teaches the concept of determining a primary supervisor device for security devices by selecting security agent (SSA) which

exchanges data and commands with it's assigned SNIU or by selecting a ASM which manages the security functions for a groups of SNIUs in a defined area, -e.g. col. 3, lines 30);

sending a single copy of the security control information to the determined supervisor device (Boyle teaches this concept by having a Security Manager (SM) which distributes security functions to SSA (SNIU security agent) –e.g. see col. 3, lines 30-42 and col. 8, lines 50-66); and

indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices (Boyle teaches this concept by having a Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to it's assigned SNIUs –e.g. see col. 3, lines 30-42 and col. 8, lines 50-66); and

aggregating the network security information generated by an indicated one of the multiple network security devices using the security control information (col. 3, lines 30-42 and col. 8, lines 50-66), by

determining at least one alternate supervisor device that stores at least a portion of the network security information generated by the indicated network security device (col. 9, lines 5-15, "alternate ASM");

notifying the primary supervisor device for the indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices (col. 9, lines 5-15, "negotiates SNIU pairings with all other ASMs"); and

in response, receiving the generated network security information, so that the manager device can efficiently distribute information to multiple network security devices, and can retrieve all of the generated network security information for a network security device because alternate supervisor devices will store the information when the primary supervisor device for the network security device is unavailable (col. 9, lines 15-23, "The SM also collets and stores the audit information generated by the SNIUs in response to the SM's criteria").

8. As to claim 2, Boyle discloses including generating network security information by (abstract), for each network security device:

monitoring network information passing between any network device in the associated group for the network security device and any network device not in the associated group (col. 6, lines55-61, col. 9, lines 15-22); and

when the monitored network information is of an indicated type col. 6, lines55-61),

determining whether the primary supervisor device for the network security device is available to receive information (col. 9, lines 5-15);

when the primary supervisor device is available, sending network security information about the monitored network information to the primary supervisor device for storage (col. 3, lines 30-42, col. 9, lines 5-22); and

when the primary supervisor device is not available, sending network security information about the monitored network information to an alternate supervisor device for storage (col. 9, lines 5-15).

9. As to claim 3, Boyle disclose wherein for each network security device, a security policy for the network security device specifies the indicated types of monitored network information for which to generate network security information and specifies data related to the monitored network information to be included in the generated network security information (col. 3, lines 30-42, col. 6, lines 15-20, col. 8, lines 50-66, col. 9, lines 5-15).

10. As to claim 4, Boyle discloses wherein the distributed security control information is software to be executed by the multiple network security devices to control the generation of the network security information (col. 11, lines 32-40).

11. As to claim 6, Boyle discloses wherein after the notifying of the primary supervisor device, the primary supervisor device sends the generated network security information to the manager device (abstract) by:

retrieving from each of the determined alternate supervisor devices the network security information generated by the indicated network security device (col. 9, lines 5-15);

retrieving any network security information generated by the indicated network security device that is stored by the primary supervisor device (col. 9, lines 15-22); and

sending the retrieved network security information to the manager device (col. 9, lines 15-22).

12. As to claim 7, Boyle discloses including after the receiving of the generated network security information, aggregating the portions of the generated network security information stored by the determined alternate supervisor devices and any portion of the generated network security information stored by the primary supervisor device (col. 9, lines 5-15).

13. As to claim 8, Boyle discloses wherein information is sent between the manager device and the supervisor devices and between the supervisor devices and the network security devices in a secure form so that others do not have access to contents of the information (col. 4, lines 45-54).

14. As to claim 9, Boyle discloses including displaying to a user the plurality of network security devices and the plurality of supervisor devices in such a manner that the primary supervisor device for each of the network security devices is visually indicated, and wherein the distributing of the security control information to the multiple network security devices is in response to selection by the user of the displayed multiple network security devices (col. 3, lines3-8).

15. As to claim 10, Boyle discloses including displaying to a user the plurality of network security devices and the plurality of supervisor devices in such a manner that the primary supervisor device for each of the network security devices is visually indicated, and wherein the aggregating of the network security information generated by an indicated one of the multiple network security devices is in response to a visual indication by the user of the one multiple network security device (col. 3, lines 3-8).

16. As to claim 31, Boyle discloses a method for distributing security policy implementation information to multiple security devices for use in implementing a security policy (abstract), the method comprising:

for each of the security devices, determining a supervisor device currently associated with the security device (Boyle Teaches the concept of determining a supervisor device for security devices by selecting security agent (SSA) which exchanges data and commands with it's assigned SNIU or by selecting a ASM which manages the security functions for a groups of SNIUs in a defined area, -e.g. col. 3, lines 30-42);

distributing the security policy implementation information to each of the determined supervisor devices (col. 3, lines 30-42, Boyle teaches this concept by distributing SM functions to SNIU security agent (SSA), area security manager (ASM) and network security manager (NSM) -e.g. col. 3, lines 30-42); and

indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor

device is associated (Boyle teaches this concept by having a Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to it's assigned SNIUs -e.g. col. 3, lines 30-42).

17. As to claim 82, it is rejected using the same rationale as for the rejection of claim 31.

18. As to claims 32 and 83, Boyle discloses wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy (col. 11, lines 32-40).

19. As to claims 35 and 86, Boyle discloses wherein the security policy implementation information is an instruction to be executed by the multiple security devices related to the implementing of the security policy (col. 11, lines 32-40).

20. As to claim 37, Boyle discloses wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation information to be distributed will replace the existing security policy implementation information (col. 3, lines 30-42, col. 8, lines 50-66).

21. As to claim 38, Boyle discloses wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation information to be distributed will supplement the existing security policy implementation information (col. 3, lines 30-42, col. 8, lines 50-66).

22. As to claim 39, Boyle discloses wherein the distributing of the security policy implementation information to each of the determined supervisor devices is performed in a manner such that the security policy implementation information is not accessible to other devices (col. 3, lines 30-42, col. 8, lines 50-66).

23. As to claims 40 and 87, Boyle discloses including displaying to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and wherein the distributing of the security policy implementation information is in response to a visual selection by the user (col. 3, lines 3-8).

24. As to claim 50, Boyle discloses a method for distributing control information to multiple security devices for use in controlling the operation of the multiple security devices (abstract), the method comprising:

for each of the security devices, determining a supervisor device currently associated with the security device (Boyle Teaches the concept of determining a

supervisor device for security devices by selecting security agent (SSA) which exchanges data and commands with it's assigned SNIU or by selecting a ASM which manages the security functions for a groups of SNIUs in a defined area, -e.g. col. 3, lines 30-42);

distributing the control information to each of the determined supervisor devices (col. 3, lines 30-42, Boyle teaches this concept by distributing SM functions to SNIU security agent (SSA), area security manager (ASM) and network security manager (NSM) -e.g. col. 3, lines 30-42); and

indicating to each of the determined supervisor devices to distribute the control information to the security devices with which the supervisor device is associated (Boyle teaches this concept by having a Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to it's assigned SNIUs -e.g. col. 3, lines 30-42).

25. As to claim 51, Boyle discloses wherein after the control information is distributed to the security devices, the security devices operate in accordance with the control information (col. 3, lines 30-42).

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 5, 33-34, 36 and 84-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle and further in view of Luckenbaugh (Patent No.: 5,991,877).

28. As to claim 5, Boyle discloses wherein the distributed security control information is a security policy that defines the network security information to be generated (abstract), and including:

after a copy of the security policy has been sent to each of the multiple network security devices, configuring each copy of the security policy with information specific to the network security device to which the security policy was sent (col. 3, lines 30-42 and col. 8, lines 50-6). Boyle doesn't explicitly disclose security control information is a security policy template. However, , Luckenbaugh discloses security control information is a security policy template (abstract, which describes "providing templates for such objects within at least one policy manager class of objects").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Boyle as taught by Luckenbaugh in order to minimize security risks by distributing standardized security policy to all devices.

29. As to claims 33 and 84, Boyle doesn't explicitly disclose wherein the security policy implementation information is a security policy template that indicates the security information to be generated. However, Luckenbaugh discloses wherein the security

policy implementation information is a security policy template that indicates the security information to be generated (abstract, which describes "providing templates for such objects within at least one policy manager class of objects").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Boyle as taught by Luckenbaugh in order to minimize security risks by distributing standardized security policy to all devices.

30. As to claims 34 and 85, Boyle discloses including: after the security policy implementation information has been distributed to each of the security devices, configuring the security policy implementation information distinctly on each security device (col. 3, lines 30-42, which describes performing configuration control to each SNIU).

31. As to claim 36, Boyle discloses wherein the security policy implementation information is information common to the multiple security devices, and wherein for each of the multiple security devices the common information is for configuring a security policy for the security device with information specific to the security device (col. 3, lines 30-42, col. 9, lines 5-15). Boyle doesn't explicitly disclose a security policy template for the security devices. However, Luckenbaugh discloses a security policy template for the security devices (abstract, which describes "providing templates for such objects within at least one policy manager class of objects").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Boyle as taught by Luckenbaugh in order to minimize security risks by distributing standardized security policy to all devices.

32. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100